

OFFICE OF THE DIRECTOR

11 Apr. 89



Office of Security

TO:

SUBJECT:

JECOM (LRMP)

- Passed Out At Today's Meeting.
- For the Files.

X

SECRET

## DCI Security Committee Goals and Objectives for 1984

- a. Develop for Community agreement a long range plan to synchronize DCI security policies and procedures for the protection of intelligence sources, methods and information based on current assessment of threats, vulnerabilities and environments.
- b. Continue efforts to enhance common Community understanding of effective security requirements and common application of DCI security policies and procedures. In support of this, seek to upgrade Community personnel clearance practices for access to non-SCI intelligence information, while ensuring that the highest standards are maintained for SCI access.
- c. Thoroughly review collection requirements on subjects of vital interest to SECOM and its subcommittees; ensure that new or revised tasking is formulated as needed. Encourage the Community to establish analysis centers to evaluate security-related data.
- d. Develop a seminar for SECOM members on personnel security studies and research; psychological profiles of spies, defectors and leakers; and innovative approaches to determining personnel reliability. Consider SECOM sponsorship of an effort to develop data on common personality traits of U.S. citizens who commit espionage.
- e. Gather anecdotal data on the value of the polygraph in personnel security screening; make sanitized material on actual cases available to those responsible for decisions on continued or expanded use of the polygraph; encourage studies of possible measures to defeat the polygraph.
- f. Develop a standard procedure for Community agencies to use in reporting to the Information Security Oversight Office on unauthorized disclosures of classified intelligence.
- g. Develop Community standards to identify and record common data on unauthorized disclosures of intelligence, seek Community agreement for a SECOM-sponsored common data base, and develop a mechanism to conduct ongoing analysis of leaks.
- h. Conduct four Community seminars each for SCI personnel, security adjudicators and for physical security officers, updating both series to keep abreast of Community needs and to enhance common application of DCI security standards.
- i. Encourage more and better use of existing security education material, such as the DCI videotape on leaks, the SECOM-developed Security Orientation for Senior Officials, and DIA videotapes on leaks and hostile espionage. Develop and produce at least one new videotape on a security education theme.

SECRET

SECRET

j. Through the SECOM Physical Security Working Group (PSWG), arrange to evaluate new physical security equipment, using the resources of the General Services Administration's Interagency Advisory Committee on Protective Equipment or the capabilities of the PSWG members, as appropriate. Establish a mechanism to approve or endorse new physical security equipment for use in protecting compartmented or classified intelligence.

k. Encourage the Community to commit more effort and resources to R&D on techniques and equipment to identify and counter hostile technical attacks. Continue to seek "seed money" for use in initiating or sustaining security R&D.

l. Complete the revision of the DCI regulation on "Security of Foreign Intelligence Information in Automated Systems and Networks" taking full account of the results of Dr. Ruth Davis's study.

m. Continue to coordinate Community support to the FBI's efforts to assist in enhancing technical security on Capitol Hill.

SECRET